The Software Alliance

BSA

March 6, 2019

The Honorable Jim Inhofe
Chairman
Senate Armed Service Committee
205 Russell Senate Office Building
Washington, DC 20510

The Honorable Jack Reed
Ranking Member
Senate Armed Service Committee
728 Hart Senate Office Building
Washington, DC 20510

The Honorable Adam Smith
Chairman
House Armed Service Committee
2264 Rayburn House Office Building
Washington, DC 20515

The Honorable Mac Thornberry
Ranking Member
House Armed Service Committee
2208 Rayburn Office Building
Washington, DC 20515

Dear Chairmen Inhofe and Smith and Ranking Members Reed and Thornberry:

As you prepare to develop the *Fiscal Year 2020 National Defense Authorization Act* (FY20 NDAA), we write to you to offer the perspective of the software industry on key legislative efforts we believe could improve our national security and enhance the ability of the Department of Defense (DoD) to innovate.

BSA | The Software Alliance (BSA) is the leading trade association representing the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, developing cutting-edge solutions in use across the range of information technology (IT) platforms, and are global leaders in advancing best practices for developing quality, secure, trustworthy software. As such, our members share the interests of the DoD and the Armed Services Committee in ensuring the highest standards of cybersecurity, driving agile and meaningful innovation, and harnessing emerging technologies.

Both as the Federal Government's largest department and as the government's leading innovator of security technologies, DoD is well positioned to play a leading role in setting policy courses in relation to software development, cybersecurity, and workforce development that can serve as examples to the rest of the government and beyond. We are therefore eager to work with you to ensure that Congress and the Department leverage this leadership opportunity and craft policies that advance security, innovation, and competitiveness simultaneously. To that end, we wish to share with you our priorities for the FY20 NDAA.

Software Acquisition and Security. We are aware that the Department of Defense is undertaking a number of efforts to address software acquisition practices, including implementation of a recent Defense Science Board report and completion of a Defense Innovation Board Software Acquisition Practices study, and that Congress is closely monitoring these efforts. We applaud both Congress and the Department for considering ways to improve software acquisition practices and encourage the Committee to take action in this year's authorization to advance these efforts. Specifically, the FY20 NDAA should:

- *Embrace best-in-class commercial solutions*. DoD has often experienced cost overruns and performance issues when it has sought to develop custom-built software to address functions that readily available commercial off-the-shelf (COTS) solutions can already provide. For many DoD use cases, a COTS solution offers the best state-of-the-art solution, quicker time-to-mission, and at lower cost than custom-built software. In approaching software acquisition reform, the Committee should establish a clear, mandatory preference for best-in-class COTS software where such software can meet the Department's requirements.
- *Improve coordination with industry on requirements development*. One way to ensure that DoD can get the best value for its money and can take advantage of the speed, agility, and innovation associated with best-in-class COTS solutions is to ensure that the requirements development process defines functional and performance requirements in ways that make sense in a commercial context. The Committee should establish a mechanism to seek industry input into, and feedback on, requirements development for software acquisitions.
- *Ensure that security is integrated throughout the software acquisition lifecycle*. Building secure software is paramount to the Department's overall cybersecurity posture. A recent Government Accountability Office (GAO) study found "mission-critical cyber vulnerabilities in nearly all weapon systems that were under development." To prevent such vulnerabilities in the future, the Department must begin to integrate security considerations throughout the software acquisition lifecycle, from program design to end-of-life. To that end, the Committee should consider requiring all software development or acquisition programs to articulate a secure development lifecycle during contract competition or program inception; likewise, the Committee should consider requiring the development of security metrics, such as defect density, to assess performance of software acquisition programs.
- *Modernize the Department's approach to software acquisition*. BSA strongly supports efforts by the Defense Innovation Board, Defense Science Board, and other key stakeholders to develop recommendations that would enable the Department to embrace more modern approaches to software development, such as Agile or DevOps development processes. In the FY20 NDAA, the Committee should (1) embrace these efforts; (2) invest in building common infrastructure to support modern software development; (3) ensure that software development infrastructure integrates security both through tools and configurations; and (4) ensure that modernizing software acquisition includes both enhancing the Department's approach to software development and improving its ability to embrace modern commercial software products and partners.
- *Train for security*. Finally, a key component to the success of efforts to modernize the Department's software acquisition processes will be a workforce that is trained in

such practices. To ensure that security remains a key focus of software development, large software developers, such as BSA's members, have found it effective to establish dedicated teams to train software developers in secure development practices. In the FY20 NDAA, the Committee should authorize the establishment of a security training element to deliver training in secure software development across the Department's software acquisition enterprise.

Supply Chain Security. We are aware that the Department of Defense, like the broader Federal Government, is wrestling with how to best secure its supply chain against malicious threats and inadvertent risks. Supply chain security is among the most pressing challenges we face in the technology sector; as the recent "Deliver Uncompromised" report from the MITRE Corporation explains, "Adversaries seek to counter areas of U.S. military dominance and to challenge U.S. interests in cyber domains via supply chains upon which our government, our industries, and our populace rely." Yet, as this statement acknowledges, supply chains are intrinsically interconnected, linking governments, businesses, and citizens across global boundaries. As a result, effective approaches to supply chain security must balance the priority of averting adversarial threats to supply chains and the imperative of sustaining global commerce and consumer trust.

BSA believes that there is a need for new public policy solutions to supply chain security, and that the DoD and the Armed Services Committees are well positioned to assume leadership in this arena. Doing so requires a careful, transparent, multi-stakeholder process to understand the impact of potential courses of action across the broad array of actors impacted by supply chain interventions. While BSA recommends a deliberate process to enable such an approach, Congress can begin this process with several potential actions in the FY20 NDAA that would reinforce both security and economic priorities. Specifically, the FY20 NDAA should:

- Embrace internationally recognized, industry driven standards for security throughout the digital supply chain. The bill should direct DoD to identify internationally-recognized, industry driven standards (such as ISO/IEC 27036) for driving security and enforce these standards throughout its digital supply chain. Such standards should, at minimum, require the enforcement of identity and access management policies, the encryption of sensitive data in transit and at rest, and continuous protection of products, systems and services through updates, upgrades and patches.
- Enforce security standards through vendor contracts. The bill should require that acquisition contracts enforce security standards, based on industry best practices, for contractors and subcontractors. Vendors should ensure that their products are maintained with currently available upgrades and patches and developed according to secure lifecycle development approaches.
- Establish procedures for transparency and appeal under the Section 881 of the Fiscal Year 2019 NDAA. Section 881 of the FY19 NDAA permanently extended authorities originally passed in Section 806 of the FY 2011 NDAA. These authorities give the department potent tools to defend against supply chain risks during acquisitions; however, they also provide for a process that can be opaque. There is a risk that such opaque processes could drive non-risk management-based protectionist interventions by governments in foreign markets, undermining the economic competitiveness of global businesses and inhibiting responsive security

behavior by DoD vendors. We recommend that Section 881 be clarified to require processes to, absent exceptional circumstances, notify vendors excluded from a competition of their exclusion and the reasons for it and to ensure a viable means of protesting or appealing the exclusion decision. Such processes can improve transparency without undermining the potency of the Section 881 tools.

- Support research and development into technologies that can foster supply chain integrity. There is also an opportunity for the Department to lead in the supply chain security arena by investing in the research and development of new technological approaches to fostering supply chain integrity. Promising areas of research include the use of blockchain-based technologies, development of processes to vet third-party components for security issues, and the application of artificial intelligence for the analysis of supply chain data and anomaly detection, among others. The FY20 NDAA should dedicate funding specifically for research and development into supply chain technologies through partnerships with academic institutions and other technology leaders.
- State U.S. policy that the Department will refrain from systemic interventions in global supply chains. Enhancing supply chain security means, in part, developing a more secure global cybersecurity ecosystem that recognizes norms for responsible behavior and prioritizes collective defense against malicious threats. The Congress can send an important message by stating that it is the policy of the United States that the Department will not undertake systemic interventions in global supply chains in connection with its Title 10 defense responsibilities.
- Avoid unnecessary isolationist approaches. We are aware of some efforts to advocate for solutions to technology development that would seek to deny foreign adversaries influence by adopting indiscriminate prohibitions against the acquisition or integration of software components developed in certain foreign nations or by certain foreign nationals. Such approaches, without any grounding in risk management, are deeply flawed. In practice, they could undermine the Department's ability to harness innovative software products, including many open source products, fundamentally undermining DoD's technological edge. Meanwhile, any security benefit could easily be achieved through more sophisticated approaches, such as the enforcement of secure software development practices. Such indiscriminate proposals should be rejected.

In addition to considering these recommendations as the Committee develops the FY20 NDAA, we urge the Committee to maintain rigorous oversight of the DoD's implementation of key provisions of last year's NDAA relating to supply chain security, including Sections 889, 1654, and 1655. BSA supports Congress's efforts to ensure the security and integrity of the US Government's supply chains but believes continued oversight of the implementation of these provisions is important to prevent unintentional consequences for responsible developers and customers of technology solutions. BSA looks forward to working with the Committee to ensure that the Department's implementation is transparent, that it solicits and incorporates feedback from impacted stakeholders, and that it advances models for software assurance that operate effectively in a global context.

Workforce Development. The evolution of the digital economy has brought tremendous new opportunities for skilled workers; according to the Bureau of Labor Statistics, software-related jobs are projected to be among the fastest growing career fields in the U.S. over the next five to ten years. Filling these jobs has created a rapidly growing demand for workers with relevant technology skills. Often military personnel and military families represent relatively untapped reservoirs of these skills. We believe there is an opportunity to empower military spouses and military personnel who have decided to transition out of service to attain relevant skills or credentials and help build the workforce of the future. To harness this potential, the FY20 NDAA should:

- *Empower military spouses*. Minimal investments in providing skills-based training opportunities to military spouses and ensuring they have access to work environments that enable them to meet job demands, can pay big dividends with regard to helping military spouses – among the most disproportionately underemployed populations in America – attain quality, well-paying software-related jobs. Specifically, the Committee should consider opportunities to develop public-private partnerships to deliver training to spouses and assess access of spouses to appropriate remote work environments (including access to broadband internet service and, partnerships with private organizations to enable access to independent work spaces, as well as arrangements under Status of Forces agreements impacting the ability of spouses stationed overseas to work).
- *Enhance opportunities for transitioning military personnel*. Military personnel who have decided to transition out of service are eligible for a range of awareness and training programs, such as the Transition Assistance Program (TAP) and Career Skills Program (CSP). Yet, these opportunities often do little to prepare transitioning personnel to acquire specific technical skills or credentials that can help them transition into technology-related careers. As the Department increasingly seeks to partner with the technology industry on innovative technological breakthroughs, both individual transitioning personnel and DoD as a whole would benefit from expanding opportunities for military personnel to transition into the technology industry and related fields. To that end, the Committee should examine opportunities to improve transition programs, such as TAP and CSP, to help transitioning personnel acquire key technical skills and credentials, obtain relevant apprenticeships and other transitional opportunities, and connect with potential employers in the technology sector.

We would welcome the opportunity to work with you and your staff to address these ideas in the FY20 NDAA. Working together, we can forge a deeper partnership between Congress, DoD, and the technology sector to advance national security and foster transformative innovation.

Thank you for your leadership, and we look forward to working with you.

Sincerely,

Craig Albright
Vice President, Legislative Strategy